

### **REMARKS**

Claims 1, 3-6, and 9-13 stand rejected under §103 on the basis of Kimlinger et al. '952, Comerford et al. '413, and Proust et al. '014. The independent claims have been amended to more clearly define the present invention over the cited references.

More particularly, the independent claims have been clarified to provide that the access control unit manages the application allowed exclusive access by the exclusion control unit to access the smart card. Applicant traverses the rejection because Kimlinger and Comerford cannot be fairly combined to achieve the advantages of the present invention. Proust does not address exclusion control of access to a plurality of applications in the manner of the present invention, or address problems relating to process IDs, as in the present invention.

The Examiner asserts that Kimlinger discloses an access management system, and Comerford discloses the feature of the present invention that the exclusion control unit controls access to the smart card from other applications. However, as described in previous comments, the parts cited by the Examiner do not disclose the exclusion control unit or the access control unit of the present invention.

Moreover, even if Kimlinger discloses the access control unit and Comerford discloses the exclusion control unit as the Examiner has argued, the simple combination of these references does not result in the present invention.

According to the present invention, an application accessing a smart card first issues a request to the exclusion control unit for exclusive access. The access control unit

then checks whether the application allowed the exclusive access by the exclusion control unit is authorized.

Thus, as shown in Fig. 4, the present invention uses both an exclusion control unit and an access control unit. The invention executes the steps of a) obtaining an exclusive access from the exclusion control unit, b) checking authorization of the application allowed the exclusive access by the exclusion control unit, and c) accessing data. With the present invention, setting/cancellation of the authentication status does not have to be conducted with each switching of a plurality of applications.

This advantageous result is achieved by using both the exclusion control unit and access control unit at the same time, and by accessing data in a smart card with the above procedures. Therefore, the matter disclosed in Kimlinger et al. corresponding to the access control unit and the matter disclosed in Comerford et al. corresponding to the exclusion control unit neither can be easily combined nor can achieve the above effect.

Proust relates to access management of a SIM card of a cellular phone. The Examiner equates the process ID of an application in the present invention with the access control policy indicator in Proust. However, the access control policy indicator is the indicator for determining the access control policy depending on the types of programs accessing the SIM card, which completely differs from the process ID of the present invention.

In addition, Proust discloses nothing about exclusion control of access to a plurality of applications. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 2 and 7-8 stand rejected under §103. Applicant traverses this rejection for the reasons given with respect to independent claim 1. Withdrawal is respectfully requested.

For the foregoing reasons, Applicant believes that this case is in condition for allowance, which is respectfully requested. The examiner should call Applicant's attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By



Patrick G. Burns

Registration No. 29,367

**Customer No. 24978**

October 10, 2006

300 South Wacker Drive

Suite 2500

Chicago, Illinois 60606

Telephone: (312) 360-0080

Facsimile: (312) 360-9315